Cyber Risk Responsibilities

Utah County Indemnity Pool
August 30, 2017

Elaina M. Maragakis
Ray Quinney & Nebeker, P.C.

1

2

You don't know what you don't know

- We have a poor understanding of adversary capabilities and resources.
- We have a poor understanding of the effectiveness of cybersecurity countermeasures.
- We have a poor understanding of the consequences of a successful attack – in particular, of the extent to which exploitation of a single vulnerability can result in widespread damage to confidentiality, integrity, or availability.

Risk Management and the Cybersecurity of the U.S. Government Input to the Commission on Enhancing National Cybersecurity, Steven B. Lipner and Butler W. Lampson, available at https://www.nist.gov/sites/default/files/documents/2016/09/16/s.lipner-b.lampson_rfi_response.pdf

3

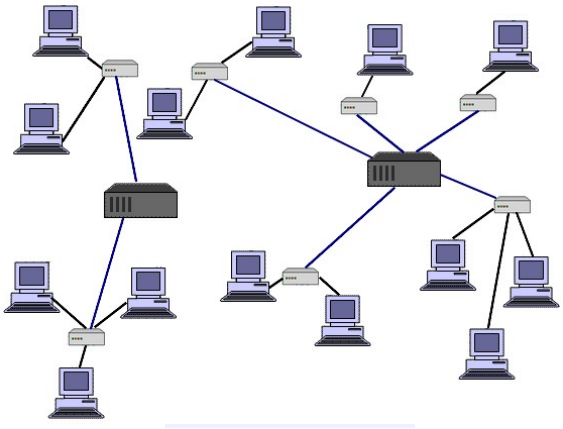
If there is a breach, are you prepared to answer the following questions:

4

Do you have a written Information Security Policy (ISP)?

5

What controls are in place?

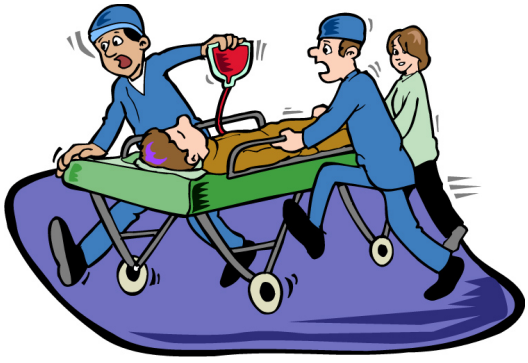


6

Do you provide any training on information security?

7

Do you have a written Data Breach Response Plan?



8

Government entities are attractive targets

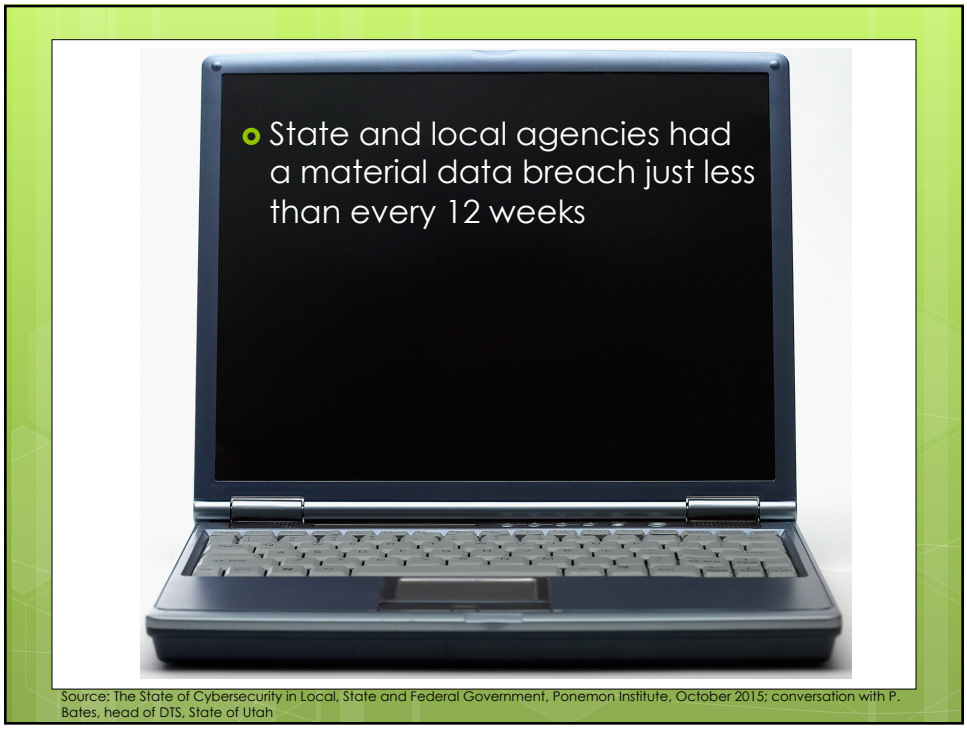
9

"There has been a huge increase in the number of attacks against state systems"

600%
over 4 month period in 2012

Source: Mathew J. Schwartz, 9 Lessons from the Utah Data Breach, 5/21/12

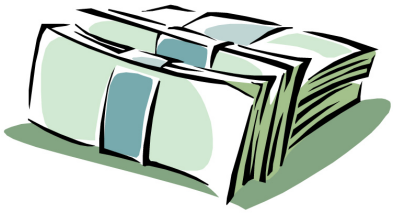
10



11

Average cost per record breached (public sector)

$68 per record



Source: Ponemon Cost of Data Breach Study: Global Analysis (May 2015)

12

Government Challenges?

13

Government Challenges

- Lack of resources
- Inadequate technology infrastructure
- Competition for security personnel
- Employee overload
- Longer time to detection and response
- Stores valuable personal information

14

Every government entity needs an

Information Security Policy

and

Data Breach Response Plan

15

Utah Protection of Personal Information Act

(1) Any person who conducts business in the state and maintains personal information shall implement and maintain reasonable procedures to:

(a) prevent unlawful use or disclosure of personal information collected or maintained in the regular course of business; and

(b) destroy, or arrange for the destruction of, records containing personal information that are not to be retained by the person.

Utah Code §13-44-201(1)

16

"The best practice for municipal government is to adopt and implement a

written information security plan"

Murtha Cullina LLP, *Cities and Towns Being Targeted by Hackers: Connecticut Municipalities Must Follow Data Breach Laws*, available at http://www.lexology.com/library/detail.aspx?g=965eea45-fe26-460f-85a9-ad26f9a71e5a, 3/31/16

17

What is an Information Security Policy?

Policy issued by an organization to ensure that users of information comply with procedures designed to secure information:

Identify
Protect
Detect
Respond
Recover

18

What is an Information Security Policy?

- **Identifies** assets and risks

19

What is an Information Security Policy?

- Creates a policy to **protect** the assets and **minimize** the risk

20

What is an Information Security Policy?

- Establishes who is responsible for **enforcement**

21

What is an Information Security Policy?

- Creates a Data Breach Response Plan

22

What is an Information Security Policy?

- **Creates a recovery plan**

23

What are the causes of data breaches?

24

Employee negligence

Every breach occurs because someone in the organization does something they shouldn't do or fails to do something they should do.

Source: Frank W. Abagnale

25

THE WALL STREET JOURNAL.

Sunday, December 20, 2015 THE WALL STREET JOURNAL.

- Thumb drives easily lost or stolen
- Out-of-office messages alert hackers when computer is not monitored
- Phishing emails to gullible employees
- Photos of work documents on phones
- Social-media posts give hackers valuable intel

Source: *The Wall Street Journal*, Sunday, December 20, 2015

26

Government Checklist

- Establish a written Information Security Plan
- Create a data breach response team
- Conduct effective employee training
- Perform regular vulnerability testing
- Review third-party vendor agreements
- Comply with PCI-DSS standards
- Start today and create a realistic timeline

27

Contact:

- Elaina M. Maragakis
Shareholder
Ray Quinney & Nebeker, PC
(801) 323-3315
emaragakis@rqn.com

28